UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/724,995	12/01/2003	Nancy Cam Winget	72255/00010	3154

23380 7590 12/03/2009
TUCKER ELLIS & WEST LLP
1150 HUNTINGTON BUILDING
925 EUCLID AVENUE
CLEVELAND, OH 44115-1414

EXAMINER	
POPHAM, JEFFREY D	

ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
12/03/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patents@tuckerellis.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/724,995
Filing Date: December 01, 2003
Appellant(s): WINGET ET AL.

Larry B. Donovan
Reg. No. 47,230
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 9/4/2009 appealing from the Office action mailed 4/10/2009.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct. It is briefly noted that there is another ground of rejection provided, adding Downnard to the combination. However, this ground of rejection was only made for dependent claims, so those rejections will stand or fall with the independent claims, as there are no further arguments. This ground of rejection is also provided below for the sake of completeness.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

2004/0268126	DOGAN	12-2004
6,978,298	KUEHR-MCLAREN	12-2005

PAUL FUNK, Simon Blake Wilson; "draft-ietf-eap-ttls-02.txt: EAP Tunneled TLS Authentication Protocol (EAP-TTLS)"; Internet-Draft PPPEXT Working Group; 30 Nov. 2002, pp. 1-40

Downnard, Ian, "Public-key cryptography extensions into Kerberos", IEEE December 2002/January 2003, pp. 30-34

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1, 2, 5, 6, 9, 10, 15-21, 24, 26, and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dogan (U.S. Patent Application Publication 2004/0268126) in view of Kuehr-McLaren (U.S. Patent 6,978,298) and Funk (PAUL FUNK, Simon Blake

Wilson; "draft-ietf-eap-ttls-02.txt: EAP Tunneled TLS Authentication Protocol (EAP-TTLS)"; Internet-Draft PPPEXT Working Group; 30 Nov. 2002, pp. 1-40).

Regarding Claim 1,

Dogan discloses a method of authenticating communication between a first and a second party, the method comprising:

Establishing a first secure tunnel between the peer and the server using asymmetric encryption if a shared secret does not exist between the two (Paragraphs 22-23);

Receiving the shared secret via the first secure tunnel between the peer and the sever responsive to the shared secret not previously existing and establishing the first secure tunnel (Paragraphs 22-23);

Tearing down the first tunnel (Figure 2A; and Paragraphs 7 and 22-24; although "tearing down" is not explicitly stated, it is clear that the registration connection is decoupled from the connections that are later opened, and that the registration connection/tunnel is terminated once the parameters discussed in paragraphs 22-23 are distributed);

Establishing a subsequent, new secure tunnel between the peer and the server using symmetric encryption and the shared secret after tearing down the first tunnel and after the peer has received the shared secret (Paragraphs 24-26);

Mutually deriving a tunnel key for the subsequent new secure tunnel using symmetric cryptography based on the shared secret responsive to establishing the subsequent, new secure tunnel (Paragraphs 24-26);

Authenticating a relationship between the peer and the server within the subsequent secure tunnel upon mutually deriving the tunnel key for the subsequent new secure tunnel (Paragraphs 24-26; this relationship is authenticated by the fact that both entities, and only those entities, can generate the connection secret); and

Cryptographically binding the subsequent new secure tunnel with conversations inside the subsequent new secure tunnel (Abstract; Figure 2A, step 208; and Paragraphs 7, 25, and 35);

But does not explicitly disclose determining whether a shared secret exists between a peer and a server.

Kuehr-McLaren, however, discloses determining whether a shared secret exists between a peer and a server (Column 6, line 29 to Column 7, line 25; and Column 11, lines 12-32). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the session management system of Kuehr-McLaren into the secret/key generation system of Dogan in order to allow the system to cache session information for a particular amount of time and dynamically modify and/or update the amount of time based upon the needs of the system and its users, thereby allowing for optimized performance while maintaining a high level of security.

Funk, however, discloses authenticating both the peer and the server to each other by means other than the mere fact that both entities can generate the correct key or secret (Pages 8-10, sections 4.1-4.3; Pages 11-13, sections 6-6.2; and Page 20, section 10). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the extensible authentication system of Funk into the secret/key generation system of Dogan as modified by Kuehr-McLaren in order to provide a number of authentication mechanisms that can be used to authenticate entities in the system, while protecting the authentication information such that it cannot be accessed by any entities that cannot derive the connection secret/tunnel key, thereby providing additional security in the system.

Regarding Claim 17,

Claim 17 is a system claim that corresponds to method claim 1 and is rejected for the same reasons.

Regarding Claim 2,

Dogan as modified by Kuehr-McLaren and Funk discloses the method of claim 1, in addition, Dogan discloses protecting the termination of the authenticated conversation by use of a tunnel encryption and authentication to protect against a denial of service by an unauthorized user (Paragraphs 22-25); and Funk discloses protecting the termination of the authenticated conversation by use of a tunnel encryption and authentication to protect against a denial of service by an unauthorized user (Pages 9-15, sections 4.3-6.4).

Regarding Claim 5,

Dogan as modified by Kuehr-McLaren and Funk discloses the method of claim 1, in addition, Dogan discloses that the shared secret is a protected access credential (Paragraphs 22-25).

Regarding Claim 20,

Claim 20 is a system claim that corresponds to method claim 5 and is rejected for the same reasons.

Regarding Claim 6,

Dogan as modified by Kuehr-McLaren and Funk discloses the method of claim 5, in addition, Dogan discloses that the protected access credential includes a protected access credential key (Paragraphs 22-25).

Regarding Claim 9,

Dogan as modified by Kuehr-McLaren and Funk discloses the method of claim 6, in addition, Funk discloses that the protected access credential includes a protected access credential opaque element (Pages 3-4, section 1; and Pages 10-13, sections 5-6.2).

Regarding Claim 10,

Dogan as modified by Kuehr-McLaren and Funk discloses the method of claim 6, in addition, Funk discloses that the protected access credential includes a protected access credential information element (Pages 11-13, sections 6-6.2).

Regarding Claim 15,

Dogan as modified by Kuehr-McLaren and Funk discloses the method of claim 1, in addition, Funk discloses that the step of authenticating is performed using EAP-GTC (Pages 21-22, section 10.2.1).

Regarding Claim 16,

Dogan as modified by Kuehr-McLaren and Funk discloses the method of claim 1, in addition, Funk discloses that the step of authenticating is performed using Microsoft MS-CHAP v2 (Pages 23-24, section 10.2.4).

Regarding Claim 18,

Dogan as modified by Kuehr-McLaren and Funk discloses the system of claim 17, in addition, Funk discloses that the communication link is a wireless network (Pages 4-5, section 2).

Regarding Claim 19,

Dogan as modified by Kuehr-McLaren and Funk discloses the system of claim 17, in addition, Funk discloses that the communication link is a wired network (Pages 4-5, section 2).

Regarding Claim 21,

Dogan as modified by Kuehr-McLaren and Funk discloses the system of claim 18, in addition, Funk discloses t hat the wireless network is an 802.11 wireless network (Pages 4-5, section 2).

Regarding Claim 24,

Dogan discloses a wireless device comprising:

A wireless network adapter for sending and receiving wireless signals with a server (Paragraphs 33-34);

Wherein the wireless device is configured to receive a shared secret from the server if no shared secret exists with the server, by establishing a first secure tunnel with the server using asymmetric encryption, receiving the shared secret via the first secure tunnel from the server, and tearing down the first secure tunnel after receiving the shared secret (Paragraphs 7, 22-24, 34, and 51);

Wherein the wireless device is configured to establish a subsequent, new secure tunnel between the wireless device and the server after the first tunnel has been torn down and if the shared secret exists by using the shared secret to mutually derive a tunnel key using symmetric cryptography based on the shared secret (Paragraphs 24-26);

Wherein the wireless device is configured to mutually authenticate with the server employing the subsequent new secure tunnel (Paragraphs 24-26); and

Wherein the wireless device is configured to derive keying material that binds the subsequent, new secure tunnel with all conversations inside the subsequent, new secure tunnel (Abstract; Figure 2A, step 208; and Paragraphs 7, 25, and 35);

But does not explicitly disclose determining whether a shared secret exists between a peer and a server.

Kuehr-McLaren, however, discloses determining whether a shared secret exists between a peer and a server, and receiving the shared secret upon determining that a shared secret does not exist with the server (Column 6, line 29 to Column 7, line 25; and Column 11, lines 12-32). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the session management system of Kuehr-McLaren into the secret/key generation system of Dogan in order to allow the system to cache session information for a particular amount of time and dynamically modify and/or update the amount of time based upon the needs of the system and its users, thereby allowing for optimized performance while maintaining a high level of security.

Funk, however, discloses authenticating both the peer and the server to each other by means other than the mere fact that both entities can generate the correct key or secret (Pages 8-10, sections 4.1-4.3; Pages 11-13, sections 6-6.2; and Page 20, section 10). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the extensible authentication system of Funk into the secret/key generation system of Dogan as modified by Kuehr-McLaren in order to provide a number of authentication mechanisms that can be used to authenticate entities in the system, while protecting the authentication information such that it cannot be accessed by any entities that cannot derive the connection secret/tunnel key, thereby providing additional security in the system.

Regarding Claim 26,

Dogan as modified by Kuehr-McLaren and Funk discloses the device of claim 24, in addition, Funk discloses that the wireless device is further configured to establish a session key seed for deriving a master session key used for mutually authenticating the wireless device employing the subsequent secure tunnel (Pages 11-16, sections 6-7).

Regarding Claim 27,

Dogan as modified by Kuehr-McLaren and Funk discloses the method of claim 1, in addition, Dogan discloses establishing a plurality of subsequent new secure tunnels between the peer and server using the shared secret (Paragraphs 7, 22-26, and claim 10).

Claims 5-10 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dogan in view of Kuehr-McLaren and Funk, further in view of Downnard (Downnard, Ian, "Public-key cryptography extensions into Kerberos", IEEE December 2002/January 2003, pp. 30-34).

Regarding Claim 5,

Dogan as modified by Kuehr-McLaren and Funk discloses the method of claim 1, in addition, Dogan discloses that the shared secret is a protected access credential (Paragraphs 22-25); but does not explicitly disclose certain aspects of such a protected access credential.

Downnard, however, discloses that the shared secret is a protected access credential (Pages 30 and 32, Kerberos and PKINIT sections). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the public-key-extended Kerberos system of Downnard into the EAP-TTLS system of Dogan as modified by Kuehr-McLaren and Funk in order to ensure authentication of entities wishing to communicate as well as a trusted party that distributes shared secret information, while improving security and scalability through use of public keys for initial authentication.

Regarding Claim 20,

Claim 20 is a system claim that corresponds to method claim 5 and is rejected for the same reasons.

Regarding Claim 6,

Dogan as modified by Kuehr-McLaren, Funk, and Downnard discloses the method of claim 5, in addition, Downnard discloses that the protected access credential includes a protected access credential key (Pages 30 and 32, Kerberos and PKINIT sections).

Regarding Claim 7,

Dogan as modified by Kuehr-McLaren, Funk, and Downnard discloses the method of claim 6, in addition, Funk discloses that the protected access credential key is a strong entropy key (Page 16, section 7); and Downnard discloses that the protected access credential key is a strong entropy key (Table 1; and Pages 30 and 32, Kerberos and PKINIT sections).

Regarding Claim 8,

Dogan as modified by Kuehr-McLaren, Funk, and Downnard discloses the method of claim 7, in addition, Downnard discloses that the entropy key is a 32-octet key (Table 1; and Pages 30 and 32, Kerberos and PKINIT sections).

Regarding Claim 9,

Dogan as modified by Kuehr-McLaren, Funk, and Downnard discloses the method of claim 6, in addition, Downnard discloses that the protected access credential includes a protected access credential opaque element (Table 1; and Pages 30 and 32, Kerberos and PKINIT sections).

Regarding Claim 10,

Dogan as modified by Kuehr-McLaren, Funk, and Downnard discloses the method of claim 6, in addition, Downnard discloses that the protected access credential includes a protected access credential information element (Table 1; and Pages 30 and 32, Kerberos and PKINIT sections).

(10) Response to Argument

Appellant argues that "Dogan does not teach or suggest cryptographically binding a subsequent secure tunnel with conversations inside the subsequent secure tunnel as recited in claim 1" (Page 11). In defining what this cryptographic binding means, Appellant states that "This means that the conversation is associated with, or tied to, the tunnel." This being the case, one of ordinary skill in the art would understand that data being encrypted and sent in this tunnel corresponds to cryptographically binding a tunnel with conversations inside the tunnel.

An explanation of how Dogan works is now provided. In Dogan, registration is first performed between the user terminal and a second device (such as a base station). During registration, a master (or shared) secret is exchanged between the two using public key cryptography. After registration, the user terminal and the base station can independently create a connection secret in order to communicate with each other in a subsequent tunnel. A connection secret will be generated using the master (or shared) secret and an initialization vector, for example. The initialization vector is not transmitted, rather it is independently generated in each device (Paragraph 31, for example). After generating the initialization vector, the devices independently generate the connection secret using the master secret and initialization vector (Paragraphs 25 and 31). Once the connection secret is generated, it is used to encrypt and decrypt communications between the devices (Paragraphs 25 and 35). This connection between the two devices corresponds the subsequent new secure tunnel of claim 1. The conversation inside the tunnel is the encrypted data being sent between the two devices. As an example, paragraph 25 of Dogan states that "for the duration of the connection, the user terminal and the base station use 208 the connection secret as the symmetric key." This connection corresponds to the tunnel as just described, the data that is communicated in this tunnel using the connection secret as a symmetric key corresponds to the conversation inside the tunnel. Paragraph 35 of Dogan goes on to describe the cryptography module of the devices in the system. Paragraph 35 teaches encrypting and decrypting data "with a cipher initialized with the connection secret generated by the secret generation module 308." This clearly fits Appellant’s definition of being associated with or tied to the tunnel, since the conversation is encrypted within the tunnel using this specific tunnel’s connection secret as the key. Therefore, encrypting (cryptographically binding) communications (conversations) inside the connection (subsequent new secure tunnel) clearly and explicitly teaches “cryptographically binding the subsequent new secure tunnel with conversations inside the subsequent new secure tunnel”.

Applicant goes on to state that “Cryptographically binding of the tunnel with the conversation inside the tunnel helps detect and prevent man-in-the-middle attacks which enable an adversary to take control of information between a peer and a server by impersonating the peer of the server." Continuing with this argument, Appellant states that "The Examiner argues that the entities of Dogan communicating inside the subsequent new secure tunnel by using the connection secret is the same as the conversation being bound to the tunnel. However, this does not detect of prevent man-in-the-middle attacks since a man-in-the-middle may impersonate a peer and begin communicating inside the tunnel." It is first noted that the claims do not refer to detecting or preventing any man-in-the-middle attack. Furthermore, no part of the application is directed to detecting man-in-the-middle attacks. Therefore, this argument about detecting man-in-the-middle attacks has nothing to do with the claims of the application. Appellant appears to argue that a man-in-the-middle may impersonate a peer within Dogan. Although such prevention of man-in-the-middle attacks is not discussed in the claims, its relevance to Dogan is now described. As described above, a terminal and base station, for example initially exchange a master (or shared) secret via public key cryptography. Paragraph 22 describes authenticating the user terminal in this registration phase, therefore, no man-in-the-middle could impersonate the terminal, as the terminal is authenticated prior to exchanging the master secret. Paragraph 23 next describes the use of public key cryptography in providing a master secret generated by the user terminal to the base station. Use of public key cryptography ensures that only the intended entity (base station) can access the master secret here. This master secret can later be used along with an initialization vector that is generated independently in each of the user terminal and base station, such that each device can independently generate the connection secret. The connection secret is then used to secure communications in the tunnel/connection. As the user terminal is authenticated, only the user terminal and base station know the master secret, and only the user terminal and base station can generate the connection secret, there is nowhere that a man-in-the-middle can impersonate a peer (this man-in-the-middle would have failed authentication and would not have the appropriate master secret and/or connection secret). The only way that a man-in-the-middle attack to work is for this man-in-the-middle to be able to acquire the appropriate parameters in order to generate the connection secret. Since only the authenticated user terminal and the base station to which the user terminal was authenticated have access to any of the parameters, this kind of attack is prevented from occurring. Furthermore, Appellant never provides any argument describing how any man-in-the-middle could perform such an attack in the system of Dogan. Due to the explicit authentication, public key usage, independent generation of connection secrets, and the fact that only the proper user terminal and base station have access to the master secret, a man-in-the-middle attack is clearly prevented. That is to say, even if an attacker were to impersonate the user terminal (e.g. by using the terminal's IP and/or MAC address), for example, the attacker would not have access to the appropriate secrets. Therefore, the attacker cannot encrypt or decrypt data using the appropriate connection secret. As the attacker cannot view or inject proper data (encrypted using the right connection secret), this form of attack is prevented.

Appellant's arguments appear to based on detecting and preventing of man-in-the-middle attacks, even though such is not discussed in the claims. Prevention of man-in-the-middle attacks is an inherent aspect of Dogan, as discussed above. However, for the sake of completeness, one may view Funk, used in rejection of claim 1. The first full paragraph on page 2 of Funk states that "EAP-TTLS allows legacy password-based authentication protocols to be used against existing authentication databases, while protecting the security of these legacy protocols against eavesdropping, man-in-the-middle and other cryptographic attacks." The final paragraph of page 3 has a corresponding paragraph. As one can see, even though not a claim limitation, Funk teaches preventing man-in-the-middle attacks. As the instant application never discusses detecting man-in-the-middle attacks, such detection is not discussed here.

Appellant provides the same arguments for claims 17 and 24, which have the same response.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Jeffrey D Popham/
Examiner, Art Unit 2437

Conferees:

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437

/Matthew B Smithers/
Primary Examiner, Art Unit 2437